DOI: 10.17803/1994-1471.2025.180.11.099-112

П. А. Скобликов*

Анализ проекта всеобъемлющей конвенции ООН против киберпреступности в контексте соблюдения прав пострадавших

Аннотация. В статье представлен анализ проекта международной конвенции против киберпреступности, который 9 августа 2024 г. был одобрен Спецкомитетом ООН по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Оценивается, как этот документ может повлиять на соблюдение прав человека, прежде всего прав лиц, пострадавших от киберпреступлений. Обнаружены пробелы и противоречия проекта, выдвинуты и обоснованы предложения по их устранению. В частности, рекомендовано убрать из проекта положения, которые вводят необоснованные преимущества для одних потерпевших в ущерб правам других. Предлагается включить в проект определения киберпреступности и киберпреступлений (представлены и обоснованы авторские дефиниции этих понятий), положения, направленные на быстрое и эффективное обжалование решений об отказе в открытии уголовного расследования по заявлению о совершенном киберпреступлении. Предложено также закрепить в проекте рекомендацию о публикации для сведения любых заинтересованных субъектов статистических данных о поступивших заявлениях о киберпреступлениях и видах предполагаемых преступных деяний, о принятых по таким заявлениям решениях и нарушении сроков рассмотрения заявлений, об обжаловании действий (бездействия) правоохранительных органов заявителями и ряд иных дополнений.

Ключевые слова: киберпреступность; киберпреступление; информационно-коммуникационные технологии; международный договор; конвенция против киберпреступности; нарушение прав человека; латентная преступность; потерпевший; пострадавший от преступления; кибермошенничество; интернет-преступление; участковый уполномоченный полиции.

Для цитирования: *Скобликов П. А.* Анализ проекта всеобъемлющей конвенции ООН против киберпреступности в контексте соблюдения прав пострадавших // Актуальные проблемы российского права. — 2025. — Т. 20. — № 11. — С. 99–112. — DOI: 10.17803/1994-1471.2025.180.11.099-112.

* *Скобликов Петр Александрович*, доктор юридических наук, ведущий научный сотрудник сектора уголовного права, уголовного процесса и криминологии Института государства и права РАН
Знаменка ул., д. 10, г. Москва, Российская Федерация, 119019
skoblikov@list.ru

Analysis of the Draft UN Comprehensive Convention against Cybercrime in the Context of Respect for the Rights of Victims

Petr A. Skoblikov, Dr. Sci. (Law), Leading Researcher, Sector for Criminal Law, Criminal Procedure and Criminology, Institute of State and Law, Russian Academy of Sciences, Moscow, Russian Federation
skoblikov@list.ru

Abstract. The paper presents an analysis of the draft international convention against cybercrime, which was approved on August 9, 2024, by the UN Ad Hoc Committee on the Development of a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes. An assessment is made of how this document may impact the observance of human rights, particularly the rights of persons affected by cybercrime. Gaps and contradictions in the project were identified, and proposals for their elimination were put forward and substantiated. In particular, it was recommended to remove the provisions that introduce unjustified advantages for some victims at the expense of the rights of others. It is proposed to include the definitions of cybercrime and cybercrimes (the author's definitions of these concepts are presented and substantiated), and to introduce provisions aimed at ensuring the rapid and effective of decisions to refuse the initiation of a criminal investigation based on a report of a committed cybercrime. The author also proposes to include in the draft a recommendation for the publication of statistical data for the information of any interested parties. This data would cover received reports of cybercrimes and the types of alleged criminal acts; decisions made on such reports; instances of missed deadlines for processing reports; and the appeal by applicants of actions (or inaction) by law enforcement agencies. A number of other additions are also proposed.

Keywords: cybercrime; cybercrimes; information and communication technology; international treaty; convention against cybercrime; human rights violation; latent crime; victim; crime survivor; cyber fraud; internet crime; district police officer.

Cite as: Skoblikov PA. Analysis of the Draft UN Comprehensive Convention against Cybercrime in the Context of Respect for the Rights of Victims. *Aktual'nye problemy rossijskogo prava.* 2025;20(11):99-112. (In Russ.). DOI: 10.17803/1994-1471.2025.180.11.099-112.

Введение

В современных реалиях киберпреступность — одна из наиболее острых проблем, с которой столкнулось человечество, она представляет значительную угрозу как для отдельно взятых государств, так и для международного сообщества в целом[1]. Причем по ряду причин эта угроза лишь нарастает, в обозримом будущем она станет еще более масштабной и сложной. Одна из этих причин — природа киберпреступности как постоянно развивающегося явления, что обусловлено быстрыми и сложными технологическими изменениями в обществе[2].

В 2019 г. Российская Федерация предложила создать профильный орган для разработки всеобъемлющей международной конвенции против киберпреступности; будущий договор призван поднять международное сотрудничество в данной сфере на качественно новый уровень. Российская инициатива получила поддержку мирового сообщества, был образован Спецкомитет ООН по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (далее — Спецкомитет ООН). Кроме того, наша страна внесла проекты резолюций, принятых

[1] *Горелик И. Б.* Формирование международно-правовой системы противодействия киберпреступности: от терминологии до проекта универсальной конвенции // Международное право. 2022. № 4. С. 61.

[2] Подробнее об этом см., например: *Brenner S. W.* Cyberthreats and the Decline of the Nation-State. Routledge, 2014.

затем Генассамблеей ООН за № 74/247 и 75/282 с целью организационно-регуляторного обеспечения деятельности Спецкомитета ООН. 27 июля 2021 г. в Вене Россия внесла в Спецкомитет ООН свой проект первого в истории универсального договора по борьбе с киберпреступностью[3].

Предложенный документ, по сути, выступает альтернативой Будапештской конвенции Совета Европы о компьютерных преступлениях от 23.11.2001. Этот договор по состоянию на начало 2025 г. являлся наиболее значимым межправительственным механизмом по борьбе с киберпреступностью: его подписали и ратифицировали 68 стран (в основном западных). Россия в договоре не участвует; есть информация, что российские представители считают Будапештскую конвенцию инструментом вмешательства во внутренние дела других государств и нарушения их суверенитета[4]. В отечественной научной литературе представлены более подробные обоснования для подобной оценки[5], хотя можно встретить и комплиментарные отзывы о данной Конвенции[6], а также критику в адрес тех государств, которые ее не подписали[7]. В любом случае за то время (четверть века), которое прошло с момента разработки документа и характеризовалось бурным развитием цифровых технологий, он серьезно устарел. Существенно и то, что Будапештская конвенция, пусть и с впечатляющим числом подписантов, всё же носит региональный характер[8].

Работу над российским проектом осложнила пандемия COVID-19 и обусловленные ею ограничения[9]. Тем не менее проект после внесения модернизировался с учетом предложений других стран и в трансформированном виде вызвал неоднозначные оценки. Постоянный представитель России при международных организациях в Вене М. Ульянов в своем телеграм-канале 10 января 2024 г. написал следующее: «После шести переговорных сессий Спецкомитета есть все основания полагать, что западники включились в переговорный процесс, имея в виду максимально размыть и выхолостить новую договоренность»[10].

Проект договора после его доработки подвергся критике и с третьей стороны, с иных позиций. Так, Раман Джит Сингх Чима, директор

---

[3] См.: О внесении в Спецкомитет ООН российского проекта универсальной международной конвенции по противодействию использованию информационно-коммуникационных технологий в преступных целях // Официальный сайт Министерства иностранных дел РФ. 28.07.2021. URL: https://www.mid.ru/ru/foreign_policy/news/1770170/ (дата обращения: 23.03.2025).

[4] *Черненко Е.* Под статью подвели не всё. Россия недовольна проектом конвенции ООН по борьбе с киберпреступностью // Коммерсантъ. 2024. 13 янв. С. 1.

[5] См., например: *Данельян А. А.* Международно-правовое регулирование киберпространства // Образование и право. 2020. № 1. С. 265.

[6] См., например: *Зверянская Л. П., Протосевич А. А.* Борьба с киберпреступностью как актуальная задача современной науки // Криминологический журнал БГУЭП. 2011. № 3. С. 28–33 ; *Шматкова Л. П.* Международное сотрудничество в борьбе с киберпреступлениями: состояние и перспективы // Молодой ученый. 2016. № 28 (132). С. 721.

[7] См., например: *Шестак В. А., Чеботарь А. С.* Будапештская конвенция как основополагающий механизм противодействия киберпреступности: новации и перспективы международно-правового регулирования // Образование и право. 2023. № 8. С. 309.

[8] Так же как и Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации, подписанное 1 июня 2001 г. в Минске.

[9] См., например: 74-я сессия Генеральной Ассамблеи ООН. Пункт 107 повестки дня «Противодействие использованию информационно-коммуникационных технологий в преступных целях» // Официальный сайт ООН. 6 августа 2020 г. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Website/A_74_L_84/A_74_L_84_R.pdf (дата обращения: 23.03.2025).

[10] См.: телеграм-канал «Михаил Ульянов». URL: https://t.me/ulyanov_mikhail/2873 (дата обращения: 23.03.2025).

по политике Access Now[11] в Азиатско-Тихоокеанском регионе, заявил, что «нынешний текст этой конвенции ослабляет стандарты в области прав человека, защищающие неприкосновенность частной жизни в цифровую эпоху, подрывая права, защищаемые конституцией Индии, как это было провозглашено нашим Верховным судом в постановлении Путтасвами в 2017 г.»[12]. Там же высказано опасение, что принятие Конвенции может в конечном итоге привести к объявлению законной онлайн-активности преступной. Это опасение высказали представители как Access Now, так и Electronic Frontier Foundation[13].

Как бы то ни было, 9 августа в Нью-Йорке Спецкомитет ООН под председательством Алжира завершил начатые два с половиной года назад переговоры принятием проекта универсального договора[14]. Этот документ[15] (далее — Проект конвенции) опубликован для всеобщего сведения на официальном сайте ООН в разделе, отведенном для освещения деятельности Спецкомитета ООН, и размещен там после текста доклада о работе его возобновленной заключительной сессии и проекта резолюции Генассамблеи ООН[16].

Свою специфику имеют потенциальные нарушения прав трех групп граждан: 1) привлекаемых к ответственности за киберпреступления; 2) пострадавших от киберпреступлений; 3) третьих лиц. В статье автор намерен проанализировать Проект конвенции с позиции соблюдения прав потерпевших, сосредоточившись на тех существенных вопросах, которые остались без внимания других аналитиков либо рассмотрены ими неполно и (или) без приведения некоторых значимых аргументов.

I. Нарушение принципа правовой определенности в Проекте конвенции и предложения по устранению неопределенности

В названии Проекта конвенции используется термин «киберпреступность», непосредственно в тексте он применяется несколько десятков раз, то есть им обозначается одно из ключевых понятий документа, но что́ есть киберпреступность — не раскрывается.

Одновременно в тексте Проекта используется термин «киберпреступление» («киберпре-

[11] Международная некоммерческая организация, которая в качестве задачи своей деятельности декларирует защиту прав граждан в цифровом пространстве. Штаб-квартира находится в Нью-Йорке (США).

[12] Это заявление цитируется в статье «Доработан договор ООН о киберпреступности: что это такое и почему ему грозит повсеместное противодействие?», опубликованной 17 августа 2024 г. в индийском издании The Indian Express. См.: *Karan Mahadik.* UN cybercrime treaty finalised: What is it and why is it facing widespread pushback? // The Indian Express. August 17, 2024.

[13] Международная некоммерческая группа по защите цифровых прав, базирующаяся в Сан-Франциско (Калифорния, США).

[14] См.: О принятии ООН проекта международной конвенции по укреплению международного сотрудничества в борьбе с информационной преступностью. 09.08.2024 // URL: https://www.mid.ru/ru/foreign_policy/news/1965185/ (дата обращения: 23.03.2025).

[15] Его полное название по состоянию на август 2024 г. громоздкое, оно состоит из заголовка и подзаголовка: «Проект конвенции Организации Объединенных Наций против киберпреступности. Укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям».
Первоначальное название (при внесении Проекта конвенции в ООН) было более лаконичным и не имело подзаголовка: «Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях». См.: URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf (дата обращения: 23.03.2025).

[16] См.: URL: https://documents.un.org/doc/undoc/gen/v24/056/77/pdf/v2405677.pdf (дата обращения: 23.03.2025).

ступления»), но там также не раскрывается, что он означает.

Такая неопределенность создает почву для произвольного толкования содержания будущего юридически значимого документа, расширения или сужения его предмета в аналогичных ситуациях, разворачивающихся в разных местах или в одном месте, но в разное время.

Поясним сказанное. Согласно положениям гл. II «Криминализация» Проекта конвенции государства-участники берут на себя обязательство принимать законодательные и иные меры, какие могут потребоваться, с тем чтобы признать в качестве уголовного правонарушения 10 определенных деяний, если они совершаются умышленно и неправомерно с использованием информационно-коммуникационных систем или электронных данных, цифровых устройств (деяния описаны в ст. 7–16). Это дает повод, в отсутствие четких ориентиров, для ограничительного толкования, а именно отнести к киберпреступлениям лишь деяния, входящие в приведенный перечень, и не более того (назовем их киберпреступлениями в узком смысле).

Вместе с тем другие положения той же главы II дают основание для более широкого толкования, при котором киберпреступлениями будут считаться все деяния, которые предлагает криминализировать Проект конвенции. Тогда помимо указанного в предыдущем абзаце к киберпреступлениям будут отнесены также деяния, предусмотренные в ст. 17; последние направлены на отмывание доходов от киберпреступлений в узком смысле, которые в данном случае являются предикатными преступлениями[17].

Ну и, наконец, следует принять во внимание, что пункт 1 ст. 4 Проекта конвенции гласит следующее: «…При осуществлении других применимых конвенций и протоколов ООН, участниками которых являются государства-участники, они обеспечивают, чтобы уголовные правонарушения, признанные таковыми в соответствии с этими конвенциями и протоколами, также *считались уголовными правонарушениями по внутреннему законодательству, если они совершаются с использованием информационно-коммуникационных-систем* (курсив наш. — *П. С.*)». Это дает повод для еще более широкого толкования киберпреступлений — как любых деяний, совершаемых с использованием информационно-коммуникационных систем.

В результате различных толкований нарушается принцип правовой определенности и могут быть ущемлены права пострадавших от соответствующих преступлений, а также граждан, привлекаемых к ответственности.

В связи с этим целесообразно включить в ст. 2 «Термины» гл. 1 Проекта конвенции разъяснения того, что есть киберпреступность и киберпреступление.

За основу предлагаем взять следующие определения:

— киберпреступность означает совокупность киберпреступлений и лиц, их совершивших (совершающих);

— киберпреступление означает уголовно наказуемое деяние, совершаемое с использованием информационно-коммуникационной системы или для получения доступа к ней, при условии что без наличия такой системы совершение данного или последующего деяния (входящего в преступный план) невозможно или существенно усложняется[18].

---

[17] Напомним, что предикатное преступление — это такое, которое является обязательным признаком объективной стороны другого преступления, по отношению к коему оно и выступает предикатным. Разновидностью предикатного преступления (предшествующим преступлением) и его классическим примером является приносящее доходы преступное деяние, если отмывание доходов от него влечет ответственность за новое (последующее) преступление — за легализацию преступного дохода.

[18] Предложенная нами дефиниция учитывает широкое по своему содержанию определение термина «информационно-коммуникационная система», сформулированное в п. «а» ст. 2 Проекта конвенции: это любое устройство или группа соединенных или взаимосвязанных устройств, одно или несколько из которых по команде программы производит сбор, хранение и автоматическую обработку электронных данных.

II. О проблеме доступа к правосудию жертв киберпреступности

В преамбуле Проекта конвенции справедливо и уместно признается важность обеспечения правосудия для жертв киберпреступности. В развитие этого тезиса в п. 2 ст. 34 Проекта конвенции включено положение о том, что «каждое Государство-участник, при условии соблюдения своего внутреннего законодательства, устанавливает надлежащие процедуры для обеспечения доступа к компенсации и возмещению ущерба потерпевшим от преступлений, признанных таковыми в соответствии с настоящей Конвенцией». Там же, в п. 2 ст. 52, содержится положение, обеспечивающее реализацию предыдущего: «Государства-участники в той мере, в какой это допускается внутренним законодательством, и в случае получения соответствующей просьбы в первоочередном порядке рассматривают вопрос о возвращении конфискованных доходов от преступлений или имущества запрашивающему Государству-участнику, с тем чтобы оно могло *предоставить компенсацию потерпевшим от преступления или возвратить такие доходы от преступлений или имущество их прежним законным собственникам* (выделено нами. — *П. С.*)».

Однако все эти и другие меры, направленные на защиту прав и интересов потерпевшего, невозможно реализовать, если потерпевший не получает доступа к правосудию, если уголовное расследование по его заявлению не возбуждается или возбуждается с большой задержкой, отчего следы преступления утрачиваются, а равно если в случае начала уголовного расследования не принимаются необходимые и своевременные меры для раскрытия преступления, закрепления его следов, обнаружения и задержания виновных, поиска похищенного имущества. На минимизацию этих проблем Проект конвенции государства-участников не ориентирует.

Между тем, как показывают некоторые социологические и криминологические исследования, проведенные в России, заявления о кибермошенничествах, о незаконном копировании персональных данных из компьютерных систем и им подобные правоохранительными органами зачастую рассматриваются по существу с большой задержкой, проверка таких заявлений обычно поручается участковым уполномоченным полиции, не имеющим необходимых навыков и умений, ресурсов и полномочий для расследования данного рода преступлений. А по заявлениям об указанных преступлениях часто выносятся постановления об отказе в возбуждении уголовного дела без надлежащих оснований.

III. Проблемы надлежащего реагирования правоохранительных органов на заявления о кибермошенничествах. Краткий анализ российской практики

Проблема безнаказанности кибермошенничества обсуждается в социальных сетях. Вот один из показательных примеров, который был опубликован 2 ноября 2024 г. телеграм-каналом «МИГ России» (у канала более чем 500 тыс. подписчиков) в рамках инициативного проекта «Народная профилактика интернет-мошенничества».

Читатель телеграм-канала рассказал, что не так давно был взломан его аккаунт на портале «Госуслуги» и от его имени оформлен, а затем получен микрозаем. Пострадавший узнал об этом только от работников отдела взыскания займодателя, поскольку в свой аккаунт заходил редко. Гражданин обратился в полицию с заявлением о мошенничестве и с претензией к микрофинансовой организации. Получив обращение пострадавшего с предложением провести проверку по данному факту и уведомление об обращении пострадавшего в полицию, микрофинансовая организация сняла свои требования. Он этим удовлетворен, хотя и получил из полиции постановление об отказе в возбуждении уголовного дела. Негативное решение никто не обжаловал[19]. Гражданин не счел нужным это делать, поскольку финансовые

[19] См.: URL: https://t.me/mig41/37772 (дата обращения: 23.03.2025).

требования к нему сняты; он сделал выводы и ведет себя теперь более бдительно[20]. Микрофинансовая организация же, вероятно, не хочет ссориться с правоохранительным органом и (или) считает, что втягивание ее в длительный и малоперспективный юридический процесс будет финансово убыточно: услуги юриста стоят дороже, чем размер выданного займа, притом что даже возбуждение уголовного дела не гарантирует последующего обнаружения злоумышленников и возмещения причиненного ущерба. Кроме того, риск непогашения некоторой части долгов заложен в повышенную процентную ставку по займам микрофинансовой организации. В итоге так или иначе страдают многие другие граждане — те, против кого продолжают совершать подобные преступления неразоблаченные преступники, и заемщики, которые выплачивают повышенные проценты по своим долгам.

Здесь полезно привести данные, предоставленные журналистам руководителем Фонда поддержки пострадавших от преступлений. Эта организация функционирует в России без малого 20 лет и оказывает бесплатную юридическую помощь пострадавшим от преступлений. В 2023 г. в Фонд поступило свыше 4 тыс. обращений, из них 70 % — от лиц, которые пострадали в результате действий мошенников. В свою очередь, среди мошенничеств, с которыми столкнулись пострадавшие, лидируют телефонные мошенничества и другие деяния, которые совершаются с использованием информационных технологий. Потерпевшие обращались в правоохранительные органы, но столкнулись там с отказами в возбуждении уголовных дел[21]. В большинстве случаев с участием юристов Фонда потерпевшим удалось добиться возбуждения уголовных дел, но обычно такие дела остаются нераскрытыми, что неудивительно — ведь время упущено; наибольшие шансы на раскрытие имеются тогда, когда работа оперативных сотрудников и следователей проводится по горячим следам, а не спустя месяцы и более.

Подробный анализ практики реагирования отечественных правоохранительных органов на сообщения о совершении киберпреступлений представлен в другой статье автора[22].

IV. О высокой латентности киберпреступности и целесообразности учета этого обстоятельства в Проекте конвенции

С 1 по 10 октября 2024 г. один из крупнейших российских банков — ВТБ — провел опрос, в котором приняли участие 1,5 тыс. человек в возрасте от 18 до 65 лет в городах России с населением более 100 тыс. человек. Согласно результатам этого опроса, в 2024 г. около 60 % россиян столкнулись с мошенничеством по телефону или в Интернете, при этом 7 % россиян попались на уловки кибермошенников. Если экстраполировать полученные результаты на всё взрослое население страны[23], то можно обоснованно предположить, что жертвами кибер-

[20] Так, помимо изложенного, гражданин обнаружил, что те же злоумышленники активировали через его кабинет на портале «Госуслуги» три СИМ-карты, которые, по всей видимости, используют в преступных схемах (карты данного оператора связи продаются без предъявления документов, персональные данные пользователя запрашиваются лишь при активации карт). Все «левые» карты он аннулировал и теперь регулярно проверяет свой аккаунт.

[21] См.: *Русова С.* Полный иммунитет // Совершенно секретно. 2024. 11 нояб. URL: https://www.sovsekretno.ru/articles/bezopasnost/polnyy-immunitet/ (дата обращения: 23.03.2025).

[22] *Скобликов П. А.* Стратегия борьбы с киберпреступностью: должное и сущее // Сибирское юридическое обозрение. 2025. Т. 22. № 1. С. 128–146.

[23] По данным Федеральной службы государственной статистики, взрослое население России на 1 января 2024 г. составило 119 305 000 человек (84 711 500 — трудоспособное население плюс 34 593 500 — лица старше трудоспособного возраста). См.: Численность населения Российской Федерации по полу и возрасту // Официальный сайт Федеральной службы государственной статистики. URL: https://rosstat.gov.ru/compendium/document/13284 (дата обращения: 05.11.2024).

мошенничеств за девять месяцев 2024 г. стали более 8 350 тыс. россиян. Между тем, согласно статистике ГИАЦ МВД России, всего в России за девять месяцев 2024 г. зарегистрировано лишь около 282 тыс. кибермошенничеств[24], то есть в 30 раз меньше.

Сколько в действительности заявлений о кибермошенничествах принято правоохранительными органами России в 2024 г. и ранее, установить сложно, ГИАЦ МВД России эти данные в открытом доступе не публикует. Не публикуются и сведения о принятых заявлениях об иных киберпреступлениях, о вынесенных по ним процессуальных решениях.

Самая общая информация об отказах в возбуждении уголовного дела (их количестве в целом безотносительно к характеру совершенного деяния и тому, как деяние квалифицировал потерпевший либо его юрист) публиковалась в России до 2014 г. включительно. Тогда в целом за год было вынесено 6 665 368 таких решений[25]. Затем эта статистика стала недоступной.

Проблема необоснованных и незаконных отказов в возбуждении уголовных дел — одна из самых серьезных и масштабных среди всех проблем, с которыми сталкиваются граждане при попытках получить уголовно-правовую защиту у государства от общественно опасных деяний. Проблема эта давняя, по некоторым причинам, описанным в юридической литературе, она приобрела массовое распространение в 1983 г. и обусловлена такими мотивами правоохранителей, как стремление снизить нагрузку, улучшить формальные показатели своей деятельности, а также коррупцией и рядом иных соображений[26]. Приемы и уловки, наработанные недобросовестными и злонамеренными правоохранителями при воспрепятствовании возбуждению уголовных дел о традиционных преступлениях, оказались востребованными при поступлении в правоохранительные органы сообщений об относительно новых преступных деяниях — киберпреступлениях, поскольку соответствующие мотивы появляются и в этих случаях, более того, они возникают чаще и могут становиться сильнее.

В 2023 г. в целом по России зарегистрировано 677 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что почти на 30 % больше, чем за аналогичный период предыдущего года. В общем числе зарегистрированных киберпреступлений удельный вес увеличился за то же время с 26,5 % до 34,8 %[27]. Эти данные показывают несостоятельность высказанного в 2020 г. прогноза, согласно которому прирост киберпреступности в России замедлится, «так как, исходя из зарубежного опыта, удельный вес киберпреступности в 30 % является на настоящее время предельным»[28]. На самом деле очерченные пределы давно пройдены, латентная часть киберпреступности в десятки (возможно, даже в сотни) раз превышает ее регистрируемую часть, поэтому правильно говорить не о пределах распространения киберпреступности, а о пределах ее выявления и регистрации, а также о пределах того, на какой массив информации о преступности способны отреагировать правоохранительная и судебная системы в соответствии с

[24] См.: Состояние преступности в России за январь — сентябрь 2024 г. С. 28 // Официальный сайт МВД России. URL: https://xn--b1aew.xn--p1ai/reports/item/56672721/ (дата обращения: 23.03.2025).

[25] См.: Состояние преступности в России за январь — декабрь 2014 года. С. 4 // Официальный сайт МВД России. URL: https://xn--b1aew.xn--p1ai/upload/site1/document_file/pxOrdPt4BF.pdf (дата обращения: 23.03.2025).

[26] См.: *Скобликов П. А.* Мотивы необоснованных и незаконных отказов в возбуждении уголовных дел // Уголовный процесс. 2013. № 4. С. 68–74.

[27] См.: Состояние преступности в России за январь — декабрь 2023 года. С. 3 // Официальный сайт МВД России. URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (дата обращения: 23.03.2025).

[28] *Кириленко В. П., Алексеев Г. В.* Гармонизация российского уголовного законодательства о противодействии киберпреступности с правовыми стандартами Совета Европы // Всероссийский криминологический журнал. 2020. Т. 14. № 6. С. 901.

действующим антикриминальным законодательством.

Принимая во внимание всё изложенное, предлагаем дополнить статью 34 «Помощь потерпевшим и их защита» Проекта конвенции двумя пунктами:

— «Каждое Государство-участник обеспечивает возможность быстрого и эффективного обжалования решения об отказе в открытии уголовного расследования по заявлению о совершенном киберпреступлении»;

— «Государства-участники рассматривают возможность публикации для сведения соответствующих международных организаций, неправительственных организаций, исследователей и других субъектов гражданского общества статистических данных относительно поступивших заявлений о киберпреступлениях и видах предполагаемых в них преступных деяний, о принятых решениях по таким заявлениям и о нарушении сроков рассмотрения заявлений, а также об обжаловании действий (бездействия) правоохранительных органов заявителями».

Точности ради заметим, что пункт 2 ст. 55 Проекта конвенции рекомендует государствам-участникам рассмотреть возможность накопления статданных, аналитических знаний и информации о киберпреступлениях для прямого и опосредованного обмена с целью выработки, насколько это возможно, общих определений, стандартов, методологий и оптимальных видов практики в деле предупреждения таких преступлений и борьбы с ними. Однако если по заявлению потерпевшего о киберпреступлении в возбуждении уголовного дела отказано со ссылкой на отсутствие события или состава преступления, то описанные в заявлениях деяния не берутся на учет и не отражаются в уголовной статистике. Иными словами, пункт 2 ст. 55 Проекта конвенции здесь неприменим.

В завершение рассмотрения данного вопроса отметим, что, по результатам недавнего исследования, осуществленного группой специалистов под эгидой Оксфордского университета, Россия возглавила рейтинг стран с самым высоким индексом киберпреступности[29]. Вывод для нас неоднозначный[30], но следует согласиться с другим, а именно: в России один из самых высоких в мире уровней цифровизации жизни (это относится и к государственному, и к частному секторам), что объективно благоприятствует распространению киберпреступности, и крайне высокий уровень преступлений, совершаемых с использованием информационно-коммуникационных технологий. А коли так, то негативный опыт России по борьбе с киберпреступлениями должен быть учтен в положениях Проекта конвенции; то, с чем столкнулась наша страна, через некоторое время придет и в другие страны, для которых проблема киберпреступности пока не стоит столь остро.

V. О соблюдении равенства жертв киберпреступлений при получении защиты со стороны государственных органов

В преамбулу Проекта конвенции включено следующее положение: «…Признавая важность учета *гендерных факторов* (выделено нами. — *П. С.*) во всей соответствующей деятельности по предупреждению преступлений, охватываемых настоящей Конвенцией, и борьбе с ними в соответствии с внутренним законодательством…

[29] Mapping the global geography of cybercrime with the World Cybercrime Index / M. Bruce [et al.] // PLOS One. April 10, 2024. URL: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0297312 (дата обращения: 23.03.2025).

[30] Он вызывает сомнение по нескольким обстоятельствам: 1) авторы исследования трактуют киберпреступность очень узко — как деятельность хакеров; 2) авторы исследования понимают, что хакеры обычно используют специальные программы, дабы избежать обнаружения, замести цифровые следы, при этом многие действуют, организуя атаки не из стран своего происхождения или постоянного проживания; тем не менее исследователи доверяют мнениям опрошенных ими экспертов, полагая, видимо, что у последних есть некие точные и конфиденциальные источники относительно принадлежности неразоблаченных хакеров к той или иной стране; 3) в исследовании неявно предполагается, что главным образом хакеры

согласились о нижеследующем…». Вероятно, в развитие этого положения в п. h ст. 53 Проекта конвенции включена рекомендация применять такие меры предупреждения киберпреступлений, как «разработка, в соответствии с внутренним законодательством, стратегий и политики предотвращения и искоренения *гендерного насилия* (выделено нами. — *П. С.*), совершаемого с использованием информационно-коммуникационной системы, а также учет при разработке мер по предупреждению особых обстоятельств и потребностей лиц, находящихся в уязвимом положении».

Термин «насилие» в Проекте конвенции используется лишь единожды — в процитированном случае, и что он означает в этом документе, не разъясняется. Причем слова и выражения «убийство», «угроза убийством», «угроза причинения вреда здоровью», «угроза сексуального насилия» и их синонимы в Проекте конвенции не используются.

В российской правовой доктрине и правоприменительной практике под насилием подразумевается применение физической силы (физическое насилие) к жертве или высказывание угрозы применения таковой (психическое насилие)[31]. Если, допустим, кому-то высказывается угроза убийством в связи с его гендерной принадлежностью и для доведения угрозы до жертвы используется информационно-коммуникационная система, то такая угроза не более опасна, чем аналогичная угроза, переданная человеку в связи с его расовой или национальной принадлежностью либо гражданством. Отсюда можно заключить, что в Проекте конвенции безосновательно проводится политика, направленная на установление неравенства потерпевших, которые пострадали (или могут пострадать) от тождественных преступлений. Предлагается усилить защиту одних потерпевших в ущерб другим: ведь ресурсы любой правоохранительной системы ограничены, и если повышенное внимание уделяется отдельной группе потерпевших, то меньшее внимание уделяется другим группам потерпевших.

Отсюда можно заключить, что рассматриваемые положения Проекта конвенции входят в противоречие с Всеобщей декларацией прав человека[32], ее статьями 1, 2 и 8[33].

VI. Об удалении из Проекта конвенции ложного приоритета

Что понимают под термином «гендерное насилие» инициаторы внесения пункта h в ст. 53

направляют свои атаки не на страны своего происхождения или постоянного проживания, а за их пределы; 4) за публикацию в журнале PLOS One авторы платят 1 495 долл. США, что вызывает некоторый скепсис относительно беспристрастности исследователей.

31 Так, крупный советский и российский правовед Л. Д. Гаухман определял насилие как «общественно опасное, противоправное воздействие на организм человека, совершенное против его воли» (*Гаухман Л. Д.* Борьба с насильственными посягательствами. М. : Юрид. лит., 1969. С. 6). Другой видный отечественный правовед, Л. Л. Кругликов, полагает, что «насилие есть физическое воздействие (причинение вреда здоровью, удары, толчки, запирание и т.п.), а также угроза применения только физического воздействия» (Уголовное право России. Общая часть / отв. ред. проф. Л. Л. Кругликов. М. : Бек, 1999. С. 84). Подобное понимание насилия представлено и в иных учебных курсах, научно-практических комментариях.

32 Принята резолюцией 217 A (III) Генеральной Ассамблеи ООН от 10.12.1948.

33 В статье 1 провозглашается равенство прав людей. В статье 2 указано, что каждый человек должен обладать всеми правами и свободами, провозглашенными рассматриваемой Декларацией, без какого бы то ни было различия из-за расы, цвета кожи, пола, языка, религии, политических или иных убеждений, национального или социального происхождения, имущественного, сословного или другого положения. И, как гарантия предыдущих положений, в ст. 8 закреплено, что каждый человек имеет право на эффективное восстановление в правах компетентными национальными судами в случаях нарушения его основных прав, предоставленных ему конституцией или законом.

Проекта конвенции в рассматриваемой редакции? Почему они уклонились от раскрытия содержания данного понятия? Не смогли его сформулировать или по какой-то причине не захотели это делать? За ответами обратимся к некоторым документам ООН, отобранным нами в ходе целевого мониторинга.

Совещание группы экспертов, созванное подразделением ООН по вопросам гендерного равенства и расширения прав и возможностей женщин, опиралось на определение, предложенное в 2018 г. специальным докладчиком по вопросу о насилии в отношении женщин, его причинах и последствиях. Согласно ему, гендерное насилие с использованием технологий есть «любое действие, которое совершается с использованием информационно-коммуникационных технологий или других цифровых инструментов, сопровождается или усугубляется их использованием или приобретает в связи с таким использованием бóльшие масштабы, причиняя или потенциально причиняя физический, сексуальный, психологический, социальный, политический или экономический ущерб или приводя к иным нарушениям прав и свобод»[34].

При этом в докладе Генерального секретаря ООН, названном «Активизация усилий в целях искоренения всех форм насилия в отношении женщин и девочек: насилие в отношении женщин и девочек, совершаемое с использованием технологий» и представленном на 79-й сессии Генеральной Ассамблеи ООН 8 октября 2024 г., отмечается, что у термина «насилие в отношении женщин и девочек в цифровых контекстах» (приводятся синонимы этого термина: «онлайн-насилие», «цифровое насилие», «кибернасилие» и др.) всё еще нет устоявшегося определения[35]. Докладчик сообщил, что он ориентируется на определение, сформулированное в резолюции 77/193 Генеральной Ассамблеи ООН[36]: «”насилие в отношении женщин и девочек” означает любой акт насилия[37], в частности сексуально или гендерно мотивированный, который причиняет или может причинить страдания женщинам и девочкам или нанести вред их физическому, сексуальному и психическому здоровью или материальному положению, а также угрозы совершения таких актов, принуждение или произвольное лишение свободы, будь то в публичной или частной сфере, в реальной жизни или в виртуальном пространстве», — и отмечает «экономический и социальный вред такого насилия».

Если обобщить приведенные определения и учесть пояснения, сделанные в процитированных документах, то можно заключить, что под *гендерным насилием*, совершаемым с использованием информационно-коммуникационной системы, инициаторы соответствующего дополнения к Проекту конвенции имели в виду любое действие, нацеленное на опорочивание[38], оскорбление или домогательство женщин и девочек, а равно их шантаж, злоупотребление доверием, принуждение к

[34] UN-Women. Technology-facilitated violence against women: towards a common definition. Report of the meeting of the expert group. New York. November 2022. P. 4.

[35] URL: https://www.unwomen.org/sites/default/files/2024-10/a-79-500-sg-report-ending-violence-against-women-and-girls-2024-ru.pdf (дата обращения: 23.03.2025).

[36] Резолюция озаглавлена «Активизация усилий в целях предотвращения и искоренения всех форм насилия в отношении женщин и девочек: гендерные стереотипы и негативные социальные нормы», принята 15 декабря 2022 г. URL: http://gender.cawater-info.net/publications/pdf/n2275962.pdf (дата обращения: 23.03.2025).

[37] Сразу заметим, что это определение является тавтологическим, оно демонстрирует распространенную логическую ошибку, порочный круг, когда определяющий термин есть повторение определяемого (насилие определяется через акт насилия).

[38] В упомянутом выше докладе Генерального секретаря ООН утверждается, что «наиболее распространенными формами направленного против женщин гендерного насилия в Интернете являются ложная информация и диффамация». Там же отмечается, что среди других наиболее распространенных форм — кибердомогательство, разжигание ненависти, выдача себя за другого, хакерство и преследование.

какому-либо действию или бездействию, причиняющие либо могущие причинить жертвам любой вред (психологический, сексуальный, экономический, политический и т.д.). Всевозможные действия, имеющие разную юридическую природу и порой диаметрально противоположные (насилие и обман, злоупотребление доверием и клевета, сексуально-виртуальное домогательство и экономическая эксплуатация) названы проводниками соответствующей идеи словом «насилие»; вероятно, это сделано для эмоционального воздействия на слушателей и читателей, успешной вербовки новых сторонников и последователей.

Таким образом, в отсутствие сколько-нибудь серьезных криминологических обоснований происходит смешение, отождествление и подмена юридических понятий, нарушение правил формальной логики, перенаправление правовой политики на ложные цели в ущерб актуальным задачам и вызовам времени.

В связи с изложенным предлагаем изъять из преамбулы Проекта конвенции указание на важность учета гендерных факторов, а из п. h ст. 53 удалить эксклюзивную рекомендацию по разработке стратегий и политики предотвращения и искоренения гендерного насилия.

Вполне достаточно того, что в п. 5 ст. 34 «Помощь потерпевшим и их защита» содержится следующее положение: «При применении положений пунктов 2–4 настоящей статьи каждое Государство-участник принимает во внимание возраст, пол и особые обстоятельства и потребности потерпевших, включая особые обстоятельства и потребности детей».

VII. О расширении круга лиц, обладающих повышенной уязвимостью для киберпреступлений, и усилении их защиты

Вместе с тем полагаем, что процитированный выше пункт 5 ст. 34 Проекта конвенции нуждается в дополнении: целесообразно после слова «детей» через запятую вставить словосочетание «а равно пожилых людей, прежде всего одиноких».

Данное предложение обусловлено повышенной уязвимостью указанной категории людей, которые, с одной стороны, по причине своей недостаточной цифровой грамотности, ослабленной памяти, интеллекта, повышенной внушаемости и прочего более уязвимы, чаще других страдают от мошенничеств и других хищений, совершаемых с использованием информационно-телекоммуникационных систем, а с другой — будучи в силу возраста ослабленными морально и физически, тяжело переживают последствия преступлений; не менее важно, что по причине утраты трудоспособности или ограничений в занятии трудом они не могут самостоятельно восстановить те имущественные потери, которые понесли[39].

Заключение

Бурное развитие цифровых устройств, информационно-коммуникационных технологий, их проникновение во все сферы жизни современного человека при многих достоинствах этих процессов имеет и обратную сторону: создается благодатная почва для такого же бурного развития, распространения и масштабирования новой формы общественно опасных деяний — киберпреступности. Киберпреступность имеет ярко выраженный транснациональный

[39] Указанные закономерности, к сожалению, проявляют себя по отношению к пожилым людям в любых странах, сколь бы благополучными и просвещенными они ни были. Так, по данным Федерального бюро расследований, в США в 2021 г. выявлено 92 тыс. пожилых людей, пострадавших от телефонных мошенничеств, которые потеряли таким образом 1,7 млрд долл. США; это на 74 % больше, чем в предыдущем году. См.: *Keiper A., Spunt D., Chiaramonte P.* FBI raises flag on elder fraud after thousands of retirees are scammed out of $1.7 billion // Fox29. October 11, 2022. URL: https://www.fox29.com/news/fbi-raises-flag-elder-fraud-thousands-retirees-scammed-1-7-billion (дата обращения: 25.03.2025).

характер прежде всего потому, что осуществляется в глобальных электронных сетях. При совершении киберпреступлений соучастники могут располагаться в разных странах, орудия и средства совершения этих преступлений могут размещаться за пределами тех правопорядков, где пребывают преступники, их жертвы в то же время могут находиться в третьих странах и, наконец, отмывание и использование преступных доходов может происходить в местах, отличных от всего указанного выше.

При таком положении объективно требуется формирование эффективных международно-правовых (глобальных и региональных) механизмов противодействия преступности в сфере информационно-коммуникационных технологий. В основе данных механизмов должны лежать хорошо продуманные и выверенные международные договоры. Автор надеется, что высказанные и обоснованные в статье замечания, установки и предложения окажутся полезными как для осмысления и улучшения рассматриваемого Проекта конвенции, ее совершенствования после подписания заинтересованными странами, так и для разработки новых документов такой же направленности.

БИБЛИОГРАФИЯ

1. *Гаухман Л. Д.* Борьба с насильственными посягательствами. — М. : Юрид. лит., 1969. — 120 с.
2. *Горелик И. Б.* Формирование международно-правовой системы противодействия киберпреступности: от терминологии до проекта универсальной конвенции // Международное право. — 2022. — № 4. — С. 60–71.
3. *Данельян А. А.* Международно-правовое регулирование киберпространства // Образование и право. — 2020. — № 1. — С. 261–269.
4. *Зверянская Л. П.*, *Протосевич А. А.* Борьба с киберпреступностью как актуальная задача современной науки // Криминологический журнал БГУЭП. — 2011. — № 3. — С. 28–33.
5. *Кириленко В. П.*, *Алексеев Г. В.* Гармонизация российского уголовного законодательства о противодействии киберпреступности с правовыми стандартами Совета Европы // Всероссийский криминологический журнал. — 2020. — Т. 14. — № 6. — С. 898–913.
6. *Скобликов П. А.* Мотивы необоснованных и незаконных отказов в возбуждении уголовных дел // Уголовный процесс. — 2013. — № 4. — С. 68–74.
7. *Скобликов П. А.* Противодействие правоохранителей возбуждению уголовных дел: система типичных приемов и уловок // Закон. — 2016. — № 7. — С. 92–105.
8. *Скобликов П. А.* Стратегия борьбы с киберпреступностью: должное и сущее // Сибирское юридическое обозрение. — 2025. — Т. 22. — № 1. — С. 128–146. — DOI: https://doi.org/10.19073/2658-7602-2025-22-1-128-146.
9. Уголовное право России. Общая часть / отв. ред. проф. Л. Л. Кругликов. — М. : Бек, 1999. — 559 с.
10. *Шестак В. А.*, *Чеботарь А. С.* Будапештская конвенция как основополагающий механизм противодействия киберпреступности: новации и перспективы международно-правового регулирования // Образование и право. — 2023. — № 8. — С. 305–310.
11. *Шматкова Л. П.* Международное сотрудничество в борьбе с киберпреступлениями: состояние и перспективы // Молодой ученый. — 2016. — № 28 (132). — С. 720–723.
12. *Brenner S. W.* Cyberthreats and the Decline of the Nation-State. — Routledge, 2014.
13. Mapping the global geography of cybercrime with the World Cybercrime Index / M. Bruce [et al.] // PLOS One. — April 10, 2024. — URL: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0297312 (дата обращения: 23.03.2025).

Материал поступил в редакцию 25 марта 2025 г.

REFERENCES (TRANSLITERATION)

1. Gaukhman L. D. Borba s nasilstvennymi posyagatelstvami. — M.: Yurid. lit., 1969. — 120 s.
2. Gorelik I. B. Formirovanie mezhdunarodno-pravovoy sistemy protivodeystviya kiberprestupnosti: ot terminologii do proekta universalnoy konventsii // Mezhdunarodnoe pravo. — 2022. — № 4. — S. 60–71.
3. Danelyan A. A. Mezhdunarodno-pravovoe regulirovanie kiberprostranstva // Obrazovanie i pravo. — 2020. — № 1. — S. 261–269.
4. Zveryanskaya L. P., Protosevich A. A. Borba s kiberprestupnostyu kak aktualnaya zadacha sovremennoy nauki // Kriminologicheskiy zhurnal BGUEP. — 2011. — № 3. — S. 28–33.
5. Kirilenko V. P., Alekseev G. V. Garmonizatsiya rossiyskogo ugolovnogo zakonodatelstva o protivodeystvii kiberprestupnosti s pravovymi standartami Soveta Evropy // Vserossiyskiy kriminologicheskiy zhurnal. — 2020. — T. 14. — № 6. — S. 898–913.
6. Skoblikov P. A. Motivy neobosnovannykh i nezakonnykh otkazov v vozbuzhdenii ugolovnykh del // Ugolovnyy protsess. — 2013. — № 4. — S. 68–74.
7. Skoblikov P. A. Protivodeystvie pravookhraniteley vozbuzhdeniyu ugolovnykh del: sistema tipichnykh priemov i ulovok // Zakon. — 2016. — № 7. — S. 92–105.
8. Skoblikov P. A. Strategiya borby s kiberprestupnostyu: dolzhnoe i sushchee // Sibirskoe yuridicheskoe obozrenie. — 2025. — T. 22. — № 1. — S. 128–146. — DOI: https://doi.org/10.19073/2658-7602-2025-22-1-128-146.
9. Ugolovnoe pravo Rossii. Obshchaya chast / otv. red. prof. L. L. Kruglikov. — M.: Bek, 1999. — 559 s.
10. Shestak V. A., Chebotar A. S. Budapeshtskaya konventsiya kak osnovopolagayushchiy mekhanizm protivodeystviya kiberprestupnosti: novatsii i perspektivy mezhdunarodno-pravovogo regulirovaniya // Obrazovanie i pravo. — 2023. — № 8. — S. 305–310.
11. Shmatkova L. P. Mezhdunarodnoe sotrudnichestvo v borbe s kiberprestupleniyami: sostoyanie i perspektivy // Molodoy uchenyy. — 2016. — № 28 (132). — S. 720–723.
12. Brenner S. W. Cyberthreats and the Decline of the Nation-State. — Routledge, 2014.
13. Mapping the global geography of cybercrime with the World Cybercrime Index / M. Bruce [et al.] // PLOS One. — April 10, 2024. — URL: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0297312 (data obrashcheniya: 23.03.2025).